

АППАРАТНО-ПРОГРАММНЫЙ ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ, СОПРЯГАЕМЫЙ С КОМПЬЮТЕРОМ ТИПА IBM PC

А.В. Димаки, А.А. Светлаков

Томский государственный университет систем управления и радиоэлектроники
E-mail: dav18@yandex.ru

Представлен аппаратно-программный генератор случайных чисел. Назначение данного устройства – генерация последовательностей случайных чисел с заданными статистическими характеристиками. В качестве источника случайных чисел используется аperiodический и непредсказуемый физический процесс – тепловой шум р-п-перехода стабилитрона. Сопряжение аппаратной части генератора случайных чисел с ЭВМ осуществляется при помощи интерфейса ISA. Приводятся результаты исследований статистических свойств последовательностей, полученных при помощи данного генератора, а также предлагается ряд мер по его совершенствованию.

1. Введение

В современных задачах моделирования различных процессов и объектов, подверженных воздействию различного ряда случайных факторов, часто требуется получение последовательностей случайных чисел. Случайные числа, входящие в данную последовательность, должны соответствовать требованиям исследуемого процесса или объекта и условиям их функционирования, т.е. быть распределены по определенному закону, иметь определенный диапазон изменения, заданные значения математического ожидания, дисперсии, и т.д. В этой связи возникает потребность создания универсального генератора случайных чисел, позволяющего получать случайные числа, удовлетворяющие вышеперечисленным условиям. В данной работе представлен разработанный авторами аппаратно-программный генератор случайных чисел, выполненный в виде периферийного устройства IBM-совместимого компьютера. Используемый в предлагаемом устройстве интерфейс ISA позволяет включать аппаратно-программный генератор случайных чисел в архитектуру большинства современных ЭВМ.

2. Анализ существующих методов получения случайных чисел

В настоящее время к решению задачи получения случайных чисел существует три основных подхода: 1) использование таблиц случайных чисел; 2) генерирование случайных чисел при помощи некоторого алгоритма и 3) использование специальных аппаратных устройств – датчиков случайных чисел [1]. Отметим наиболее существенные достоинства и недостатки вышеперечисленных подходов.

При наличии достаточно обширной таблицы случайных чисел вопрос об источнике независимых реализаций случайной величины можно считать принципиально решенным. Однако на практике хранение обширной таблицы в памяти вычислительной машины представляется крайне неудобным, и таблицы случайных чисел не используются, за очень редкими исключениями. Также, к недостаткам применения таблиц случайных чисел относится тот факт, что таблицы существуют для весьма ограниченного набора законов распределения.

В практических расчетах наиболее удобно получать реализации случайной величины при помощи некоторого алгоритма. Числа, получаемые таким путем,

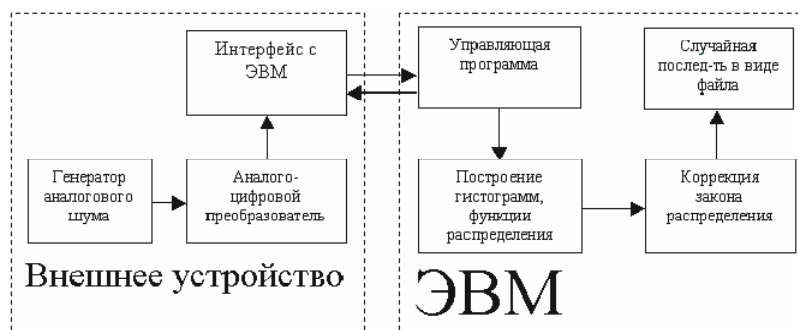


Рис. 1. Структура аппаратно-программного генератора случайных чисел

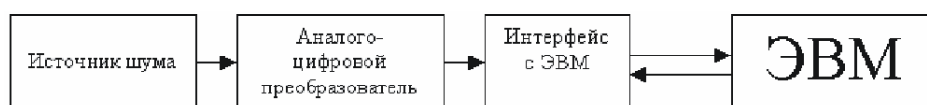


Рис. 2. Аппаратная часть генератора случайных чисел

называют псевдослучайными. Основным требованием, предъявляемым к подобным алгоритмам, является, как правило, требование высокого быстродействия.

Поддаляющее большинство используемых псевдослучайных последовательностей получают на основе рекуррентных соотношений. Однако, подобные последовательности являются периодическими, так как каждое последующее число такой последовательности определяется на основании некоторой комбинации предыдущих значений. Таким образом, использование псевдослучайных чисел позволяет получать последовательности, распределенные по требуемому закону, однако эти последовательности неизбежно будут периодическими и, в конечном счете, предсказуемыми.

От данного недостатка свободны устройства, называемые аппаратными или физическими датчиками случайных чисел. Такой датчик подключается к ЭВМ и выдает случайное число в память машины. Отличительной особенностью подобных устройств является то, что генерируемые ими случайные числа являются, по сути, измеренными значениями какого-либо случайного физического процесса, и, вследствие этого, генерируемые датчиком последовательности значений случайной величины аperiодичны (если, конечно, аperiодичен используемый физический процесс) и непредсказуемы. К недостаткам подобного рода устройств можно отнести невозможность повторного воспроизведения вычислений, и, что более важно, возможность непредсказуемого изменения параметров устройства под влиянием внешних факторов – температуры, электрических и магнитных полей, старения элементной базы. В силу этих причин физические датчики используются достаточно редко. Необходимо отметить, что аппаратно-программные генераторы случайных чисел, выполненные путем сопряжения физического датчика и ЭВМ, свободны от недостатка, связанного с невозможностью воспроизводить вычисления. Этот недостаток устраняется путем сохранения в памяти машины полученной последовательности случайных чисел для ее повторного использования. Естественно, что

объем последовательности ограничивается объемом запоминающего устройства ЭВМ. Также, преимуществом использования ЭВМ является возможность исследования запомненных последовательностей и выяснение таких их свойств, как периодичность, предсказуемость, вид функции распределения и др. [2, 3].

В силу того, что в настоящее время большая часть моделирующих программ ориентированы на работу на платформе IBM-совместимых ЭВМ, представляется актуальным создание генератора случайных чисел как самостоятельного периферийного устройства, встраиваемого в архитектуру такого компьютера. В данной работе приведены результаты проектирования, изготовления и исследования аппаратно-программного генератора случайных чисел, подключаемого к ЭВМ при помощи интерфейса ISA.

3. Структура разработанного устройства

Разработанный генератор случайных чисел состоит из аппаратной и программной частей (рис. 1). Аппаратная часть предназначена для получения аналогового шума, его усиления и оцифровки. Программная часть управляет процессом оцифровки, принимает оцифрованный шум, хранит и обрабатывает полученную последовательность случайных чисел.

Аппаратная часть состоит из собственно источника шума, аналого-цифрового преобразователя и интерфейсной части, предназначенной для сопряжения с ЭВМ (рис. 2).

В качестве источника шума используется стабилитрон КС162А. Шум, снимаемый со стабилитрона, подается на усилитель, выполненный на двух операционных усилителях КР140УД708. Суммарный коэффициент усиления составляет 530. Усиленный сигнал подается на вход устройства выборки/хранения и затем на аналого-цифровой преобразователь (АЦП), выполненный на микросхеме КР572ПВ1. Время выборки данной микросхемы составляет 250 мкс, частота преобразования – 4 кГц. Отсчеты оцифрованного сигнала поступают в

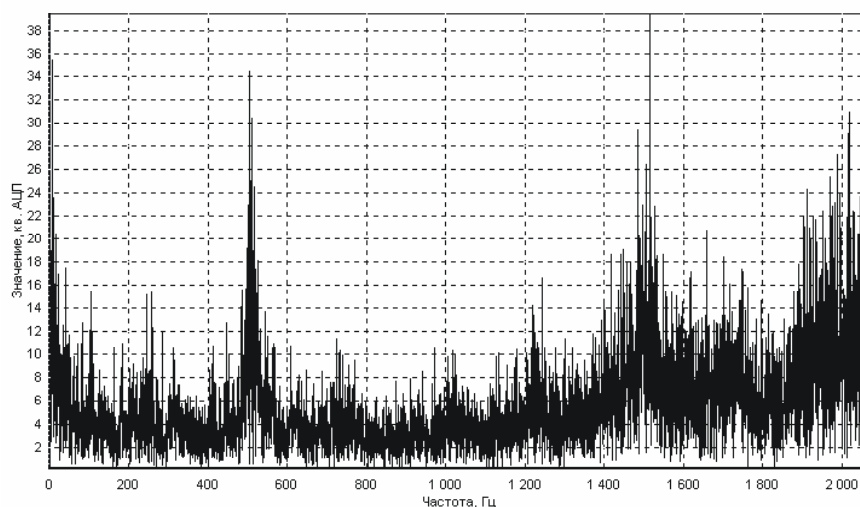


Рис. 3. Спектр шумового сигнала (N=10000)

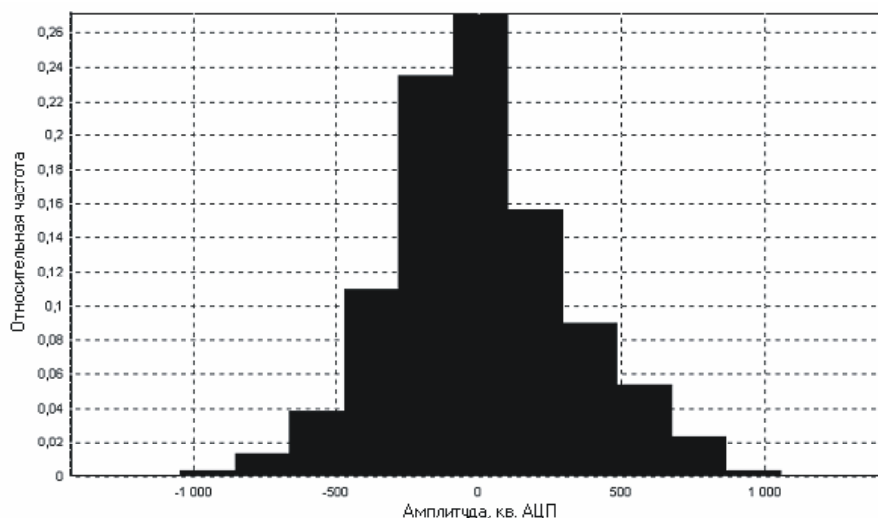


Рис. 4. Гистограмма выборки (N=10000, выборка центрирована)

ЭВМ через стандартный интерфейс ISA.

Для приема оцифрованного шума и его обработки создан специализированный пакет программ, выполняющий следующие функции:

1. Получение последовательностей значений шумового сигнала и сохранения их в виде файла.
 2. Вывод полученных последовательностей на экран в виде временных диаграмм.
 3. Построение гистограмм полученных выборок, получение числовых характеристик выборок.
 4. Построение амплитудно-частотных характеристик сигнала.
 5. Преобразование исходного закона распределения последовательности в любой из законов распределения, предусмотренных в разработанной программе.
4. Описание аппаратной части устройства

Аппаратная часть генератора случайных чисел со-

стоит из трех блоков, выполненных на единой печатной плате. К ним относятся:

1. генератор шума;
2. аналого-цифровой преобразователь;
3. интерфейс с ЭВМ.

Блок генерации шума предназначен для получения шумового сигнала – так называемого «белого шума» [4]. Отличительной особенностью такого сигнала является равномерная амплитудно-частотная характеристика. Как показано в [3], значения амплитуд такого сигнала подчиняются нормальному распределению. Таким образом, данный генератор шума позволяет получать нормально распределенные случайные числа.

Аналого-цифровой преобразователь преобразует переменное входное напряжение в двенадцатиразрядный параллельный код. При этом входному напряжению минус 3,3 В соответствует код 0, а напряжению плюс 3,3 В – код 4095. Время одного преобразования составляет примерно 250 мкс.

Использованная микросхема КР572ПВ1 представ-

ляет собой неполный АЦП, т.е. она содержит цифро-аналоговый преобразователь (ЦАП) и регистр последовательного приближения. Аналоговый компаратор, операционный усилитель ЦАП, устройство выборки и хранения, а также источник опорного напряжения монтируются отдельно.

Цифровой код, соответствующий подаваемому напряжению, хранится в регистре последовательного приближения, входящем в состав АЦП. В этот регистр поступают данные от компаратора, который сравнивает входное напряжение с опорным, вырабатываемым микросхемой КР572ПВ1. Если входное напряжение больше, то компаратор выдает высокий уровень, иначе – низкий. Таким образом, происходит последовательное формирование цифрового кода. В силу особенностей данного АЦП, преобразование сигнала происходит в нем за 27 тактов.

Рассчитаем быстродействие АЦП. С контакта OSC шины ISA поступают прямоугольные импульсы с фиксированной частотой $f_0 = 14,31818$ МГц. На двух последовательно включенных счетчиках эта частота делится на сто двадцать восемь.

$$f_1 = \frac{f_0}{128} = \frac{14,31818}{128} = 0,11186 \text{ МГц}$$

Следовательно, период импульсов на входе тактирования АЦП равен

$$T_1 = \frac{10^{-6}}{f_1} = \frac{10^{-6}}{0,11186} = 8,94 \text{ нс}$$

Так как полный цикл преобразования осуществляется за двадцать семь тактов, время преобразования равно:

$$t_{\text{цикл}} = 1 \cdot 27 \cdot 8,94 \cdot 10^{-9} = 241,4 \text{ нс}$$

Частота получения выборок сигнала равна

$$f_{\text{цикл}} = \frac{1}{t_{\text{цикл}}} = \frac{1}{241,4 \cdot 10^{-9}} = 4142 \text{ Гц}$$

Блок интерфейса с ЭВМ выполняет функцию связующего звена между аналого-цифровым преобразователем и шиной ЭВМ. Связь с ЭВМ осуществляется с использованием сигналов стандартного ISA-разъема [6]. Устройство работает в режиме побайтного обмена, используя порты ввода/вывода 0x300, 0x301. Используются только 9 младших разрядов адреса. Через порт 0x300 передается младший байт 12-разрядного кода, а 4 старших бита передаются через порт 0x301.

5. Описание программной части устройства

Программная часть разработанного устройства состоит из двух блоков – из модуля сбора данных и графического интерфейса пользователя (ГИП). Модуль сбора данных представляет собой управляющую программу, написанную на языке Си, предназначенную для приема данных из аппаратной части и записи их в файл. ГИП используется для визуализации и обработки записанных данных, а также для преобразования закона распределения полученных последовательностей.

Графический интерфейс разработан в среде Borland Delphi 5 по технологии многодокументного интерфейса (MDI) [7], т.е. в одном окне можно просматривать одно-

временно или по отдельности временную диаграмму сигнала, спектр сигнала, гистограмму. Также ГИП позволяет производить изменение исходного закона распределения на любой из законов распределения, предусмотренных в программе. В данной версии ГИП возможно преобразование исходного закона распределения последовательности в один из следующих законов распределения:

1. равномерное;
2. нормальное;
3. треугольное;
4. экспоненциальное;
5. гамма-распределение;
6. Вейбулла-Гнеденко;
7. двойное экспоненциальное;
8. бета-распределение;
9. Коши;
10. хи-квадрат-распределение.

При этом пользователь может самостоятельно задавать значения параметров любого из законов распределения.

6. Некоторые результаты исследований

Частотный спектр сигнала, получаемого с генератора шума, является важной характеристикой, позволяющей судить о наличии гармонических составляющих в шуме, наличии постоянной составляющей, а также о равномерности распределения энергии шума по частоте, т.е. о том, насколько соответствует получаемый сигнал ожидаемому «белому» шуму. Спектр сигнала, получаемого с помощью аппаратно-программного генератора, приведен на рис. 3.

Как видно из рис. 3, спектр сигнала является существенно неравномерным, в нем присутствуют ярко выраженные пики на частотах 500, 1500 и 2000 Гц. Такой вид спектра является характерным, и не изменяется от выборки к выборке. Возможно, что наличие пиков на спектре обусловлено именно типом стабилизатора, который изначально не предназначен для генерации шума. По-видимому, для получения более равномерных спектров необходимо применять специализированные диоды-генераторы шума, например, диоды КГ401А. Однако, неравномерность спектра шумового сигнала не исключает возможности его использования в качестве источника случайных чисел, так как спектр шума определяет лишь вид закона распределения получаемых случайных чисел, но не влияет на сам характер их образования как результат непредсказуемого физического процесса [8].

Типовая гистограмма выборки, получаемой при помощи генератора шума, представлена на рис. 4.

Как показывают исследования, приведенные в [8], закон распределения выборок, получаемых при помощи аппаратно-программного генератора, близок к нормальному закону распределения, математическое ожидание близко к нулю.

7. Заключение

В результате выполнения данной работы получен

аппаратно-программный генератор случайных чисел. Генератор предназначен для генерации случайных выборок необходимого объема, вид и значения параметров закона распределения которой могут быть заданы по желанию пользователя. Аппаратно-программный генератор случайных чисел может быть использован в задачах моделирования, в которых необходимы большие последовательности случайных данных, распределенных по определенному закону.

На данном этапе видны следующие возможности совершенствования разработанного аппаратно-программного комплекса:

1. Использование более совершенного шумящего элемента, имеющего спектр, более близкий к спектру белого шума.
 2. Совершенствование программного обеспечения, расширение набора законов распределения, введение функций тестирования получаемых последователь-
6. Новиков Ю.В., Калашников О.А., Гуляев С.Э. Разработка устройств сопряжения для персонального компьютера типа IBM PC. Под общ. ред. Ю.В. Новикова. Практическое пособие. – М.: ЭКОМ, 1998. – 224 с., ил.
 7. Тейксейра С., Пачеко К. Delphi 5. Руководство разработчика: Пер. с англ.: уч. пос. – М.: Издательский дом «Вильямс», 2000. – 832 с.: ил.
 8. Димаки А.В., Светлаков А.А., Сиверцев В.Ф. Разработка и некоторые результаты исследований аппаратно-программного генератора случайных чисел // Аппаратно-программные средства автоматизации технологических процессов. Под ред. Ю.А. Шурыгина. – Томск: Изд-во ТГУ, 2002. – Вып. 4. – С. 18–25.

ностей.

3. Совершенствование аппаратной части устройства, в частности повышение быстродействия АЦП, а также использование более современного интерфейса с ЭВМ.

СПИСОК ЛИТЕРАТУРЫ

1. Ермаков. С.М. Метод Монте-Карло и смежные вопросы, изд. 2-е. – М.: Наука, 1975. – 412 с.
2. Вентцель Е.С., Овчаров Л.А. Теория вероятностей и ее инженерные приложения. – М.: Наука, 1988. – 480 с.
3. Быков В.В. Цифровое моделирование в статистической радиотехнике. – М.: Советское радио, 1971. – 328 с.
4. Бобнев М.П. Генерирование случайных сигналов. – Изд. 2-е, перераб. и доп. – М.: Энергия, 1971. – 240 с.
5. Хоровиц П., Хилл У. Искусство схемотехники: В 3-х томах: Т. 1. Пер. с англ. – 4-е изд., перераб. и доп. – М.: Мир, 1993. – 413 с.